UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* WHITE 2021 BMW X5, bearing VIN 5UXCR4C07M9F79089 or California license plate 9FAY215	)	Case No. 2:24-MJ-3052

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Caption Above

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1028, 1029, 1341, and 1956	See affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Lisa Cummings

Applicant's signature

Postal Inspector Lisa Cummings

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Stephanie Christensen, U.S. Magistrate Judge

Printed name and title

AUSA Andrew Brown, x0102, 11th Floor

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1028, 1029, 1341, and 1956 (identity document and access device fraud, mail fraud, and money laundering), collectively referred to as the "SUBJECT OFFENSES"):

a. Personal identifying information of individuals other than those residing at 1027 WILSHIRE BOULEVARD, APT 536, LOS ANGELES, CA 90017, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, PINs, credit reports, and bank or other financial institution information, and records referring or relating to such information;

b. Counterfeit identity documents, such as passports and driver's licenses, whether blank, completed, or partially completed, and their components, such as seals, watermarks, security windows, official signatures or the cutting-and-pasting of signatures, holographic security features, ultraviolet printed features, raised micro dot features, and translucent Teslin printed design components, identification-proportioned photographs of faces, and programs or records referring or relating to them;

c. Blank or partially completed credit and debit cards, cards with magnetic strips that are commonly overwritten to produce counterfeit access devices, such as gift cards with no value on them (which will be determined after the search) or blank card stock, any card for which the embossing or information on the front does not match the information recorded on the magnetic strip on the back

(which will be determined after the search), any card with a PIN written on it or attached to it, lists of PINs, and records or documents referring or relating to the same;

d. Equipment designed to produce identity cards or access devices or their security features, such as card printers, embossers, encoders, magnetic card readers or writers, credit card chip readers and writers, their components and supplies, such as blank card stock, tipping foil, Teslin sheets, holographic printing supplies, ultraviolet printing supplies, and records or programs that refer or relate to them;

e. Card skimming devices and card skimming device components that attach to Automated Teller Machines (ATM) and Point of Sale (POS) terminals such as false keyboards, PIN pads, and pinhole or spy cameras;

f. Mail matter and shipping packages, opened or unopened, not addressed to or from 1027 WILSHIRE BOULEVARD, APT 536, LOS ANGELES, CA 90017, and documents or records referring or relating to the same;

g. Currency, prepaid debit or credit cards, and casino chips with a value in excess of $1,000, including the first $1,000 if more than $1,000 is found;

h. Documents and keys relating to public storage units, rental cars, prepaid cellular telephones, safety deposit boxes, Commercial Mail Receiving Agencies, or receiving mail at someone else's address;

i. Records referring or relating to counter surveillance of law enforcement, prison, arrests, criminal investigations, criminal charges, asset forfeiture, investigations by financial

institutions, and the threatened or actual closure of accounts by financial institutions;

j. Documents and records referring or relating to currency transaction reports (CTRs), their reporting thresholds, attempting to structure cash transactions to avoid CTRs, cash transactions totaling over $10,000 even if conducted in lesser increments, or the purchase of more than $3,000 of postal money orders in a two-week period, or conducting multiple cash ATM transactions or purchasing multiple postal money orders on the same day;

k. Documents and records referring or relating to the conversion of cash to financial instruments such as checks and wire transfers, and vice versa, for a percentage of the dollar value converted, or the transfer of cash abroad, such as through Hawalas or money transferring businesses, like Western Union, or the purchase of cryptocurrency for cash;

l. Records relating to wealth and the movement of wealth since January 2023, such as tax returns and forms, crypto-currency accounts and transfers, other digital wealth storage and transfer methods including PayPal and Venmo, money orders, brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, transactions involving prepaid cards, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or

showing or referring to purchases or transactions for more than $1,000;

m. Records or items containing indicia of occupancy, residency or ownership of any location or vehicle being searched, such as keys, rental agreements, leases, utility bills, identity documents, cancelled mail, and surveillance video;

n. Documents and records showing electronic and telephone contacts and numbers called or calling, such as SIM cards, address books, call histories, telephone bills, and Signal, ICQ, Telegram, and email addresses.

o. Cryptocurrency and related records and items, such as those referring or relating to public or private keys or addresses, or cryptocurrency wallets or their parts, including "recovery seeds" or "root keys" which may be used to regenerate a wallet. Seizure of the cryptocurrency and wallets will be accomplished by transferring or copying them to a public cryptocurrency address controlled by the United States, or by restoring them onto computers controlled by the United States.

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history,

user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified,

or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period

without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team will not search for similar evidence outside the scope of the items to be seized without first obtaining authority to do so.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1)itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or

copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device

8. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumbs and/or fingers of Jeremy Paul RYAN onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front

of the face of Jeremy Paul RYAN with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant, and do not apply to any other search of digital devices.

AFFIDAVIT

I, Lisa Cummings, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a United States Postal Inspector ("Postal Inspector") with the Los Angeles Division of the United States Postal Inspection Service ("USPIS") and have been so employed since August 2007. I am currently assigned to the Multi-Functional External Crimes Team at the San Bernardino Domicile. I graduated with a Bachelor of Arts Degree in International Business from San Diego State University, in San Diego, California. I am a graduate of the USPIS Career Development Unit (CDU) in Potomac, Maryland, where I completed Postal Inspector Basic Training. My responsibilities include investigating mail fraud, mail theft, identity theft, crimes against the United States Postal Service ("USPS"), crimes related to the misuse and attack of the mail system, and assaults and threats against USPS employees. As part of the 12-week residential training provided at the USPIS CDU, I successfully completed mail fraud courses detailing how mail thieves steal in various ways in order to gain access to checks, money orders, cash, gift cards, as well as personally identifiable information ("PII"). I also learned that mail thieves use this information to commit bank fraud, check fraud, and access device fraud with credit cards, debit cards, and checks stolen from the mail.

2. I have investigated crimes involving access device fraud, fraud in connection with identification documents, and Internet fraud and financial crimes. Based on my training and

experience, I am familiar with the manner in which persons engaged in identification fraud and identity theft; the manner in which those crimes are perpetrated; certain techniques, methods, or practices commonly used by persons engaged in identification fraud and identity theft activity; and indicia of cybercrime activity.

3. As a U.S. Postal Inspector, I am authorized to conduct criminal investigations, make arrests, and execute search and arrest warrants. I have participated in several multi-agency investigations involving the production of false identification documents. Specifically, vendors and fraudulent document mill operators who produce fraudulent Driver's Licenses, Passports, Social Security Cards, Permanent Resident Cards and Credit Cards.

II. PURPOSE OF AFFIDAVIT: SEARCH WARRANT

4. This affidavit is made in support of applications for a warrant to search the following:

a. 1027 WILSHIRE BLVD, APARTMENT 536, LOS ANGELES, CA 90017 and assigned TANDEM PARKING SPACE NUMBER L1-142 (the "**RYAN APARTMENT**"), as further described in Attachment A, which is incorporated by reference;

b. A GRAY 2023 AUDI E-TRON GT, bearing VIN WAUCJBFW5P7000513 and California license plate 9GSH309 or temporary California license plate CR05L88 (the "**RYAN AUDI**");

c. A WHITE 2021 BMW X5, bearing VIN 5UXCR4C07M9F79089 and California license plate 9FAY215 (the "**RYAN BMW**").

5. The requested search warrants seek authorization to seize evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1028, 1029, 1341, and 1956 (identity document and access device fraud, mail fraud, and money laundering, collectively referred to as the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

A. SUMMARY OF PROBABLE CAUSE

7. The U.S. Postal Inspection Service ("USPIS") and Homeland Security Investigations ("HSI") are investigating Jeremy Paul RYAN ("RYAN") for the manufacturing of counterfeit credit cards and identifications. RYAN has received shipments of fraudulent credit card and identification making equipment at his residence at the **RYAN APARTMENT**. The investigation further showed that RYAN, utilizing his eBay account, had purchased various fraudulent credit card and identification making equipment. RYAN has an extensive criminal history which includes identity theft, counterfeiting, and forgery.

B. RYAN HAS RECEIVED SHIPMENTS OF FRAUDULENT CREDIT CARD AND IDENTIFICATION MAKING EQUIPMENT AT HIS RESIDENCE

8. HSI Special Agent ("SA") Nick Jones, who has almost 20 years' of experience as a special agent and investigates the counterfeiting of identification documents and credit cards, reviewed records from eBay, showing that one account, later identified as being used by Jeremy RYAN ("RYAN") was purchasing credit card and identification making equipment. Specifically, eBay account Jasimp-5101 was used to purchase credit card and identification making equipment. Registration information for eBay account Jasimp-5101 listed the shipping address of 1001 Redondo Ave, Ste 3, #350, Long Beach, CA 90804 and a phone number of 562-714-4127. This address is a Private Mailbox ("PMB") at a Commercial Mail Receiving Agency ("CMRA") at a FedEx Store located at 1001 Redondo Ave, Suite 3, Long Beach, CA 90804. A CMRA is a private business that accepts mail from the USPS for others (recipients), retains it for collection (in most cases a private mailbox "PMB"), or re-mails it to another location with payment of new postage. Mail services offered by CMRAs are external to services offered by the USPS, therefore CMRA customers bear the costs associated with the services provided. Customers can rent a private mailbox ("PMB") from CMRAs.

9. From March 11, 2024 to March 30, 2024, Jasimp-5101 had numerous logins from IP: 104.60.91.96, which according to AT&T records is subscribed to JEREMY RYAN, at 1027 WILSHIRE BLVD, APT

536, LOS ANGELES, CA (the **RYAN APARTMENT**). The account was established on July 27, 2023.

10. Below is a summary of the items purchased by Jasimp-5101:

Purchase Date/Time	Seller User ID	Title
18-Nov-23	myidworld	J2A040 CHIP JAVA Cards w/ HiCo 2 Track Mag JCOP21-36K - 10 Pack Seal - Unfused
18-Nov-23	myidworld	Geniune Fargo HDP5000 84061 Color UV Ribbon - YMCFK - 500 prints - Sealed - New
18-Nov-23	myidworld	Pearl - SLE - Small Chip - HiCo 2 Track - Pack of 100
18-Nov-23	myidworld	Fargo 84053 Transfer Film for HDP5000 Printers - 1,500 Prints - Sealed - New
18-Nov-23	myidworld	100 White HiCo Mag PVC Cards, CR80 .30 mil, 3 Track Magnetic Stripe USA Shipping
30-Nov-23	ghelya	USB C To Dual HDMI Adapter USB C Docking Station 13 In 1 Triple Display USB C
30-Nov-23	yoguo-0	2.13inch E-Ink Display HAT for Raspberry Pi 4B/3B+/3B/2B/Zero/Zero W/WH,Jetso...
30-Nov-23	thanksbuyer	1MHz-6GHz SDR Radio PortaPack H2+HackRF One R9 V1.9.x +Antennas+Data Cable #USA
30-Nov-23	gatekeeper_23rd	USB 2.0 HUB 7 in 1 Docking Station USB HUB PS2 RS232 DB25 With USB Cable & PS
30-Nov-23	electrospareparts	Raspberry Pi Zero W v1.1 / PiSugar Included! - Ships From USA
24-Jan-24	incode_corp	SUPER SALE! Zebra White Sign Panel Ribbon, 1000 prints - P330i... USA Made
24-Jan-24	shulamiteliyahu	100 Pack - Premium CR80 30 Mil Graphic Quality 2 Track PVC Cards with 5/16" H...
24-Jan-24	incode_corp	Zebra Silver Semi-Dimensional Hologram Ribbon, 1000 prints - P330i - Made in USA
19-Feb-24	netac-official-store	Netac 1TB 2TB 512GB Internal SSD 2.5" SATA III 6Gb/s Solid State Drive lot
2/25/2024 0:00	mar7352	SAMSUNG EVO Plus 256GB MicroSD Micro SDXC C10 Flash Memory Card w/ SD Adapter

11. Based on SA Jones' training and experience, he is aware that many of the items listed above that were received or purchased by RYAN could be used for legitimate purposes such as generic printer parts, or unspecified ink or ribbons. However, when taken as a group in conjunction with the specialized equipment purchased by RYAN, to include: holographic printing, ultraviolet printing, embossing, laser engraving, card printing, and blank cards specifically used to make both credit cards and identifications; the use of all the equipment and materials have the combined purpose to be used to manufacture counterfeit credit cards and identifications. Ultraviolet (UV) ribbons and hologram ribbons are used to duplicate security features in credit cards and identity documents. SA Jones knows of no legitimate use for

them for a private individual. The point of ultraviolet light is that it is not visible to the naked eye, and can only be seen under special lamps designed to reveal the presence or absence of a security feature, so there is no reason for someone not engaged in counterfeiting to have the ability to print in a way that is normally invisible. Additionally, SA Jones knows from his training and experience that RYAN has possessed all the equipment and supplies necessary to manufacture both counterfeit credit cards and identifications with the variety of forged security features present on both.

12. Based on SA Jones' training and experience, he knows that "HDP5000" refers to a style of printer; furthermore, SA Jones knows that this type of printer is specifically designed for printing on PVC cards, such are used for identification and credit cards. Additionally, he knows that the HDP5000 can print ultraviolet features. Fraudulent identification and counterfeit credit card makers require ultraviolet printers in order to print the ultraviolet security features present on many IDs and credit cards. In SA Jones' experience, ultraviolet printers, their inks, and printer ribbons, used by counterfeiters are expensive, and SA Jones knows of no legitimate use for them for a private individual. The terms "Java Chip," "Small chip," and "Hico mag PVC," in SA Jones training and experience, are specific types of blank pvc cards, specifically used to manufacture identifications and credit cards. These type of chip cards, would not be used for common legitimate pvc card purposes such as novelty business cards, corporate loyalty cards, or business membership or

identification cards. Based on SA Jones' training and experience, and from speaking with other law enforcement officers, he knows that the items listed above, which RYAN recently purchased on eBay, are commonly used to produce fraudulent credit cards and identifications. Furthermore, SA Jones knows that a "hologram ribbon" is a printer ribbon used for holographic printing. The purpose of holograms is to prevent their duplication by cameras, scanners, and other equipment available to many individuals, as the resulting copy would not "move" if tilted back and forth, revealing that it is not a true hologram. Again, holograms serve as a security feature on high-value items such as credit cards and identity documents, so there is no reason for someone not engaged in counterfeiting to have the ability to print genuine holograms that will seem to move if tilted.

C. RYAN HAS MANY CONVICTIONS, INCLUDING FOR FRAUD

13. I reviewed RYAN's criminal history, which included convictions for: possession of unauthorized access devices, identity theft, receiving stolen property, possession of a controlled substance, grand theft, get credit/use others ID, and money laundering.

14. RYAN's last sentence included three years of federal supervised release, which began in August 2022. According to his Judgment and Commitment Order, he and his property are subject to search as follows:

> "The defendant shall submit his person, property, house, residence, vehicle, papers, computers [as defined in 18 U.S.C. § 1030(e)(1)], cell phones, other electronic communications or data storage devices or media, office, or other areas under his control, to a search conducted by a United States Probation

Officer or law enforcement officer. Failure to submit to a search may be grounds for revocation. The defendant shall warn any other occupants that the premises may be subject to searches pursuant to this condition. Any search pursuant to this condition will be conducted at a reasonable time and in a reasonable manner upon reasonable suspicion that the defendant has violated a condition of his supervision and that the areas to be searched contain evidence of this violation."

D. RYAN LIED TO HIS PROBATION OFFICER ABOUT HIS ADDRESS

1. RYAN Falsely Claimed to Live at the Cecil Hotel

15. On April 5, 2024, I spoke with Probation Officer Robert Gardner ("Gardner") regarding RYAN. Gardner advised that RYAN had reported approximately two weeks earlier that his current address was at the Cecil Hotel, 640 S. Main St, Apartment 828, Los Angeles, CA 90014. Gardener stated that RYAN reported that he was currently living with his friend Nicholas Stewart at the hotel. Gardner advised that RYAN never reported 1027 WILSHIRE BLVD, APT 536, LOS ANGELES, CA 90017 (the **RYAN APARTMENT**) as his address to probation. Gardner advised that RYAN stated he was in between places and sometimes stays with his girlfriend in Tustin, but he primarily lives at the Cecil Hotel in Los Angeles. Gardner stated that RYAN provided his cell phone number as (562) 230-3932.

16. On April 19, 2024, I spoke with Assistant Manager Paula Hastings ("Hastings") at the Cecil Hotel in Los Angeles. Hastings stated that RYAN does not currently reside in apartment 828 at the Cecil Hotel. She also verified that RYAN was not living in any of the apartments at the Cecil Hotel. Hastings stated that Nicholas Ray Steward currently resides in apartment 828. She stated it is a single room occupancy and no one else

lives in the unit. I also spoke with Leasing Manager Leslie Morales ("Morales") regarding RYAN. Morales stated that RYAN previously lived at the Cecil Hotel approximately one year ago, but he does not currently reside there.

17. On May 2, 2024, Gardner stated RYAN claims not to have any stable employment, and is not paying restitution because of his purported lack of income.

2. RYAN Actually Resides at a Luxury Apartment on Wilshire that he Never Disclosed to His Probation Officer

18. On April 4, 2024, the Post Office advised that Jeremy RYAN is currently receiving mail at 1027 WILSHIRE BLVD, APT 536, LOS ANGELES, CA 90017 (the **RYAN APARTMENT**).

19. I spoke to SA Jones, who informed me that RYAN has received three international packages addressed to him at the **RYAN APARTMENT**, to include most recently a package addressed to RYAN on March 23, 2024, shipped from an individual in Shenzhen, China. Based on my training and experience, many counterfeiting supplies are shipped from that area.

20. On April 17, 2024, I confirmed through USPS records that seven parcels have been delivered to RYAN or "Alex Hernandez" at the **RYAN APARTMENT** via the U.S. Mail from August 4, 2023 through February 27, 2024.

21. On April 19, 2024, I obtained a copy of the lease agreement for RYAN, 1027 WILSHIRE BLVD, APT 536, LOS ANGELES, CA 90017 (the **RYAN APARTMENT**) from leasing manager Milton O'campo ("O'campo"). Copies of RYAN's California driver's license and Mastercard credit card ending in 6817 were provided with the

lease agreement. I reviewed the lease agreement, which showed RYAN as the "guest"/resident. No other individuals were listed as residents on the lease agreement. RYAN signed the lease agreement on June 29, 2023. On the lease agreement, RYAN listed his phone number as (949) 354-7198 and his previous address of 1120 Stanley Avenue, Unit A, Long Beach, CA 90804. RYAN's vehicle was listed as a GREY 2023 AUDI E-TRON GT WITH TEMPORARY LICENSE PLATE CR05L88 (the "**RYAN AUDI**"). According to the lease agreement, RYAN pays $5,140 per month for rent. According to the rental application, RYAN works full-time as a Regional Director at De Novo Enterprises in Orem, Utah, and earns a salary of $145,000 per year, which is contrary both to his EDD wage records, discussed more later, and RYAN's statements to his probation officer that he lacked stable employment. RYAN also indicated that he earns additional income from his two vehicles. O'campo advised that RYAN also rents out his vehicles through the TURO app online and is also trying to open a "Cloud" pizza kitchen. O'campo stated that RYAN rented a two bedroom, two bath apartment and is the only person on the lease. I also spoke with Manager Vrej Torosian ("Torosian") at the security/parking office at the apartment building. Torosian advised that RYAN was assigned TANDEM PARKING SPACE NUMBER L1-142 with two parking spots for his two vehicles, which were listed as a BMW and an Audi. The license plate numbers for the BMW and Audi were not listed on the vehicle parking space information cards. RYAN's cell phone number of (949) 354-7198 was listed as an emergency phone number for RYAN on both assigned parking space cards.

Torosian stated that a white male in his 50s visits RYAN often. Torosian was unable to provide the name or a description of this individual.

22. On April 19, 2024, surveillance of the apartment building of the **RYAN APARTMENT** showed that APARTMENT 536 was located on the fifth floor. Postal Inspector Kevin Lee observed a blue Tesla with California license plate number DC46G02 (temporary tag) and a WHITE BMW SPORTS UTILITY VEHICLE ("SUV") with California license plate number 9FAY215 (the **RYAN BMW**) parked facing each other in RYAN's assigned TANDEM PARKING SPACE NUMBER L1-142 in the parking structure.

23. I reviewed Department of Motor Vehicle ("DMV") records for the WHITE BMW with California license plate number 9FAY215 (the **RYAN BMW**), which showed the registered owner was RYAN, 1120 Stanley Avenue, Unit A, Long Beach, CA 90804. The vehicle registration was suspended effective March 21, 2024.

24. I reviewed DMV records for the AUDI E-TRON GT with California license plate number CR05L88 (the **RYAN AUDI**), which showed that permanent plate number 9GSH309 had been issued and the registered owner was RYAN, 1120 Stanley Avenue, Unit A, Long Beach, CA 90804.

25. I reviewed DMV records for the blue Tesla with California license plate number DC46G02, which showed the registered owner was Mason Kane Morris, 1942 Smokewood Avenue, Fullerton, CA 92831.

26. On May 13, 2024, surveillance of the apartment building of the RYAN APARTMENT was conducted by Postal Inspectors

Michael Harrold and Michael Memoli. Inspector Harrold observed a blue Tesla and a WHITE BMW SUV parked in RYAN's assigned TANDEM PARKING SPACE NUMBER L1-142 in the parking structure. Inspector Harrold was unable to see the license plates of the vehicles.

27. In my training and experience, it is common for persons who are under court supervision to try to hide their true address from their probation officer if they are actively engaged in criminal conduct to avoid discovery of their offenses. This is especially true for criminals like RYAN who have a search condition.

C. RYAN'S FINANCIAL ACCOUNT RECEIVED PAYMENTS IN ANOTHER PERSON'S NAME

28. I reviewed bank record information for RYAN, which showed the following:

a. Venmo account XXXXX3230 is in the name JEREMY RYAN, mailing addresses: 1120 Stanley Ave Unit A, Long Beach, CA and 9411 S Central Ave, Los Angeles, CA, phone: 9493547198, and email: zapizza.oc@gmail.com. Venmo account XXXXX3300 is in the name Anthony King ("King"), mailing address of 1001 Redondo Ave, Ste 3, No. 350, Long Beach, CA 90804. Both accounts received direct deposits that Bancorp Bank flagged as fraudulent, and indicative of Automated Clearing House ("ACH") fraud. The suspicious direct deposits were received between January 2, 2023 and June 20, 2023, totaling $3,326.62; Venmo is an online payments service offered by PayPal, Inc. allowing users to link a bank account, credit card, or debit card to fund personal payments to other users. Between January 2, 2023 and June 20,

2023, RYAN and King collectively received five direct deposits totaling over $3,000. These direct deposits came from merchant names Money Network and Turo. Money Network is a service that can assist with setting up direct deposit and Turo is a car sharing platform that can send received funds via direct deposit (www.moneynetwork.com and www.help.turo.com). Some of these direct deposits had intended recipient names that were different than the named account holder. For example, RYAN received a direct deposit on June 20, 2023 for $1,230 that had the intended recipient name as "Kelly Koslowski". Additionally, Bancorp Bank has contacted Venmo stating that these direct deposits received are fraudulent. RYAN primarily used the received funds for purchases with various merchants using Venmo debit card XXXXXXXXXXXX2451.

29. HSI SA Jones reviewed telephone subscriber and call records for the phone number 949-354-7198, which is associated with RYAN's Venmo account that received the deposit in someone else's name. There was no subscriber listed for the phone number. In my training and experience, it is common for criminals to obtain telephones to use in their crimes that have no subscriber information, as it makes it harder for law enforcement to investigate their activities.

D. RYAN'S ACTUAL EMPLOYMENT INCOME IS INCONSISTENT WITH HIS LIFESTYLE

30. On April 5, 2024, I reviewed RYAN's records from the California Employment Development Department ("EDD"), which is responsible for tracking wage data. The latest wage data for

RYAN is from the last quarter of 2022 to the first quarter of 2023. During this timeframe, RYAN was employed at Urban Pie, LLC in Long Beach, CA. From the second quarter of 2023 through the first quarter of 2024, RYAN has no employment income. This is inconsistent with his current lifestyle which, as discussed previously, includes rent over $5,000 per month and multiple luxury cars.

E. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT AND COUNTERFEIT IDENTITY DOCUMENTS

31. From my training and experience, and from discussions with other investigators with dozens of years of experience investigating counterfeit identity documents and identity theft, I know the following:

a. Makers of counterfeit identity documents must maintain specialized equipment and supplies to craft convincing counterfeits of drivers licenses and other identity documents, such as card printers, cameras, raised printers, laminators, die cutters, etching equipment, scoring and cutting tools, ultra-violet printers, holographic printers, magnetic stripe and/or chip encoding devices, ink and cartridges for the required printers, pvc cards, Teslin sheets, holographic self-adhesive sheets, laminating sheets and pouches, specialized glues and adhesives, and various computers and software required to design identifications as well as operate much of the above described equipment. Much of this equipment can also be used to create counterfeit checks, credit cards, and other financial instruments, so many identity document counterfeiters are also

involved in fraud generally. Typically, criminals store such equipment and supplies where they feel it is safe and readily accessible to them, most commonly at their residence.

b. Counterfeit identity documents are often used to commit identity theft. That is, criminals purchase counterfeit identity documents so that they can impersonate particular individuals, for example to withdraw money from a bank, to negotiate a counterfeit check, or use a stolen or counterfeit credit card. In more sophisticated operations, false identity documents have been used to obtain mortgages when the criminal tricks a lender or notary into believing that the criminal is the real homeowner.

c. Individuals involved in identity theft and fraud schemes must keep evidence of their schemes, such as victim information and accounts used in the scheme, simply to keep the scheme going. Much of this evidence is now stored on digital devices such as computers and smartphones.

d. Counterfeiters of identity documents have to possess the identifying information that is to be written on the documents they will produce, such as names, drivers' license numbers, social security numbers, addresses, ID-sized photographs, signatures, and so forth. Typically, this information is transmitted and stored digitally.

e. Professional identity document counterfeiters are often paid in cash, as all those involved seek anonymity. More recently, some use cryptocurrency or peer-to-peer payment systems like Venmo or Zelle to receive their payments.

Regardless of the payment method, professional counterfeiters must keep track of which customers have paid them in order to stay in business. Commonly this is done digitally. Many professional counterfeiters will deposit some of their cash proceeds into bank accounts, or use them to purchase money orders or cryptocurrency, so that they can spend the proceeds at places that do not commonly accept cash payments, such as for rent, or store the proceeds safely.

f. Generally, perpetrators of fraud and counterfeiting schemes maintain the evidence described above where it is close at hand and safe, such as in their residences, automobiles, and, especially with smartphones, on their person. For larger or more sophisticated frauds, participants often attempt to distance themselves from some of the incriminating evidence by renting public storage units or safety deposit boxes where they often keep the items they will not need immediate access to.

g. Members of a criminal conspiracy must communicate with one another out of necessity. Commonly this is done by text, email, telephone, or specialty communication application, often an encrypted one such as WhatsApp, and most often by smartphone. Members of the conspiracy commonly carry their smartphones, which include the contact information for their co-conspirators, on or near their persons, such as in their cars or residences.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

32. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[1] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

33. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

34. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress JEREMY RYAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of JEREMY RYAN's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

35. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

VI. CONCLUSION

36. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, will be found in the RYAN APARTMENT, RYAN AUDI, and RYAN BMW.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this __ day of May, 2024.

_____

UNITED STATES MAGISTRATE JUDGE